

PATENT
Attorney Docket No. 201385
Client Reference No. 131356.01

ZFW
AF

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of:

LAMB et al.

Art Unit: 2142

Application No. 09/489,629

Examiner: VU, THONG H.

Filed: January 24, 2000

For: NETWORK ACCESS CONTROL USING
NETWORK ADDRESS TRANSLATION

**TRANSMITTAL OF
APPELLANTS' APPEAL BRIEF**

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with 37 CFR 41.37, appellants hereby submit Appellants' Brief on Appeal.

The items checked below are appropriate:

1. Status of Appellants

This application is on behalf of ☒ other than a small entity or ☐ a small entity.

2. Fee for Filing Brief on Appeal

Pursuant to 37 CFR 41.20(2), the fee for filing the Brief on Appeal is for: ☒ other than a small entity or ☐ a small entity.

Brief Fee Due \$500.00

3. Oral Hearing

☒ Appellants request an oral hearing in accordance with 37 CFR 41.47.

A separate paper requesting oral hearing is attached.

04/15/2005 EFLORES 00000009 121216 09489629

01 FC:1403 1000.00 DA



4. **Extension of Time**

- ☐ Appellants petition for a one-month extension of time under 37 CFR 1.136, the fee for which is \$ 0.00.
- ☒ Appellants believe that no extension of time is required. However, this conditional petition is being made to provide for the possibility that appellants have inadvertently overlooked the need for a petition and fee for extension of time.

Extension fee due with this request: \$

5. **Total Fee Due**

The total fee due is:

Brief on Appeal Fee	\$500.00
Request for Oral Hearing	\$1,000.00
Extension Fee (if any)	\$ 0.00

Total Fee Due: \$1,500.00

6. **Fee Payment**

- ☐ Attached is a check in the sum of \$
- ☒ Charge Account No. 12-1216 the sum of \$1,500.00. A duplicate of this transmittal is attached.

7. **Fee Deficiency.**

- ☒ If any additional fee is required in connection with this communication, charge Account No. 12-1216. A duplicate copy of this transmittal is attached.

Respectfully submitted,

Phillip M. Pippenger, Reg. No. 46,055
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza
180 North Stetson Ave., Suite 4900
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: April 11, 2005

CERTIFICATE OF MAILING

I hereby certify that this APPEAL BRIEF TRANSMITTAL AND APPEAL BRIEF (along with any documents referred to as attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Date: April 11, 2005



PATENT
Attorney Docket No. 201385

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Lamb et al.

Application No. 09/489,629

Art Unit: 2142

Filed: January 24, 2000

Examiner: Vu, Thong H.

For: NETWORK ACCESS CONTROL USING NETWORK ADDRESS
TRANSLATION

APPELLANTS' BRIEF ON APPEAL

Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In support of the appeal from the final rejection dated January 24, 2004,
Appellants now submit their Brief.

(1) Real Party In Interest

The patent application that is the subject of this appeal is assigned to Microsoft Corporation.

(2) Related Appeals and Interferences

There are no appeals or interferences that are related to this appeal.

04/15/2005 EFLORES 00000008 121216 09489629
01 FC:1402 500.00 DA



Re Appln. of Lamb, et al.
Application No. 09/489,629

(3) Status of Claims

Claims 1-33 are currently pending in this application, stand finally rejected, and are at issue herein.

(4) Status of Amendments

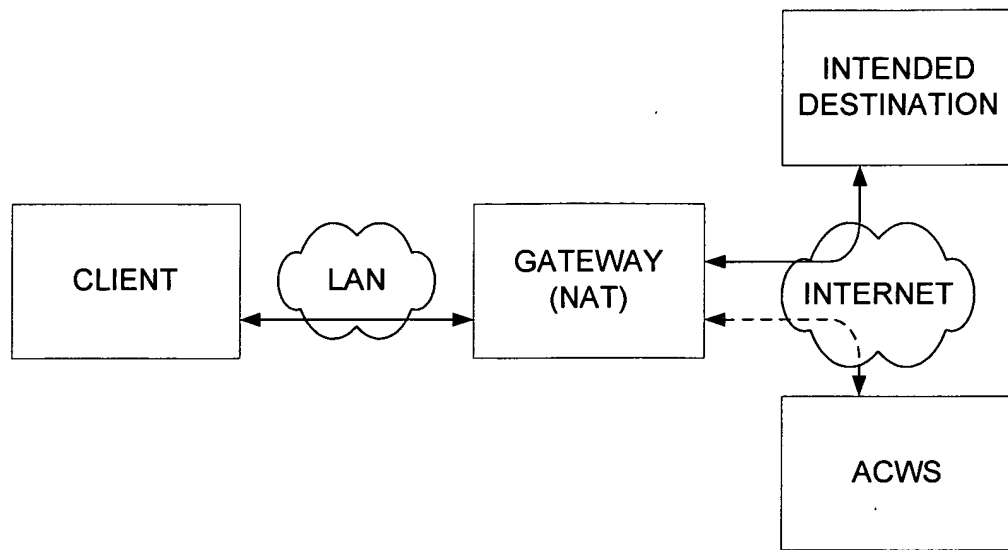
There are no outstanding amendments in this application.

(5) Summary of Invention

The present invention is directed to a system for network access control that uses Network Address Translation (NAT) capabilities to control access to material over the network. *See* page 3, line 21- page 4, line 3. Communication packets from a client on one network (e.g., a LAN) destined for a target server on another network (e.g., the Internet), are *redirected* out of the intended path at a gateway to an access control server, which then *responds* to the gateway to indicate whether access to the desired resource on the target server should be allowed. *Id. See also* Fig. 3.

If access is allowed, all subsequent packets in that session are simply inspected in real time by the gateway to determine when a connection to a different destination is attempted. *See* page 4, lines 8-10. This method operates much more efficiently than existing filtering mechanisms due to its limited intervention in an approved session, as well as its ability to function without instantiating proxies or reconfiguring clients. *See* page 4, lines 11-15. The filtering function provided by the invention is also difficult to circumvent by local client users because it does not reside or operate locally. *Id.*

For the Board's convenience, a copy of Applicants' FIG. 3 illustrating an exemplary embodiment of the invention is reproduced below without figure numbers:



It can be seen that the client communication intended for the destination server is actually initially redirected by the Gateway to an Access Controlling Web Server (ACWS). *See* Fig. 3, and page 11, lines 5-21. The ACWS will then determine whether access should be granted and instruct the Gateway to either allow or deny the communication in question. *See* page 12, lines 5-10.

The type of network access control provided by the invention can be used in any situation where a client and a server communicate over a network(s) and access control is desired; however one exemplary use is to provide access control for parents or teachers to allow them to protect children from harmful Internet content. *See* page 1, lines 17-19.

(6) Issues

The issues presented in this appeal are the following:

1. Whether claims 1, 17, and 33 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329) (hereinafter "*Gelman*").
With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation where *Gelman* does not teach or suggest all of the limitations of claims 1, 17, and 33.
2. Whether claims 2 and 18 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation where *Gelman* does not teach or suggest all of the limitations of claims 2 and 18.

3. Whether claims 3, 6, 13, 19, 22, and 29 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation where *Gelman* does not teach or suggest all of the limitations of claims 3 and 19.

4. Whether claims 4 and 20 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

5. Whether claims 5 and 21 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

6. Whether claims 8, 15, 24, and 31 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

7. Whether claims 9, 16, 25, and 32 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

8. Whether claims 10, 11, 26, and 27 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

9. Whether claims 12 and 28 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

10. Whether claims 7, 14, 23, and 30 are anticipated under 35 U.S.C. §102 by *Gelman et al* (U.S. Pat. No. 6,415,329).

With respect to this issue, a more specific question presented is whether the examiner has made out a *prima facie* case of anticipation by inherency where no reasoning, technical or otherwise, has been given to support the assertion that teachings missing from *Gelman* would have been inherent therein.

(7) Grouping of Claims

Applicants respectfully submit that the claims of this application do not stand or fall together. Specifically, the Applicants respectfully state that claims are divided into the following ten groups, the claims within each group standing or falling together:

(Group 1) claims 1, 17, and 33;

(Group 2) claims 2 and 18;
(Group 3) claims 3, 6, 13, 19, 22, and 29;
(Group 4) claims 4 and 20;
(Group 5) claims 5 and 21;
(Group 6) claims 8, 15, 24, and 31;
(Group 7) claims 9, 16, 25, and 32;
(Group 8) claims 10, 11, 26 and 27;
(Group 9) claims 12 and 28; and
(Group 10) claims 7, 14, 23, and 30.

The foregoing groupings of claims are appropriate under 37 C.F.R. § 1.192(c)(7) since each of Groups 1-10 is subjected to a different ground of rejection, as will be apparent from the argument presented herein below. Applicants have not attempted to differentiate claims within these groups.

(8) Argument

It is axiomatic that a *prima facie* case of anticipation can only be established when a single reference teaches, expressly or inherently, all limitations of the targeted claims. As will be discussed below, the Applicants respectfully submit that this basic criterion is not met by the rejection of the pending claims based on *Gelman*. In particular, several claims are rejected based on alleged teachings from *Gelman* where *Gelman* lacks the alleged teaching.¹ Moreover, the remaining claims are rejected based on teachings said to be inherent in *Gelman*, however, no reasoning for this conclusion is given, and Applicants submit that the allegedly inherent teachings are plainly not inherent in the reference. Indeed, not only do the alleged inherent teachings not flow *necessarily* from the express teachings of the reference, but in most cases, there is no reason to believe that alleged inherent teachings are even consistent with the reference's actual teachings. Therefore, the Applicants respectfully submit that the examiner has

¹ The pending claims are attached at Appendix A.

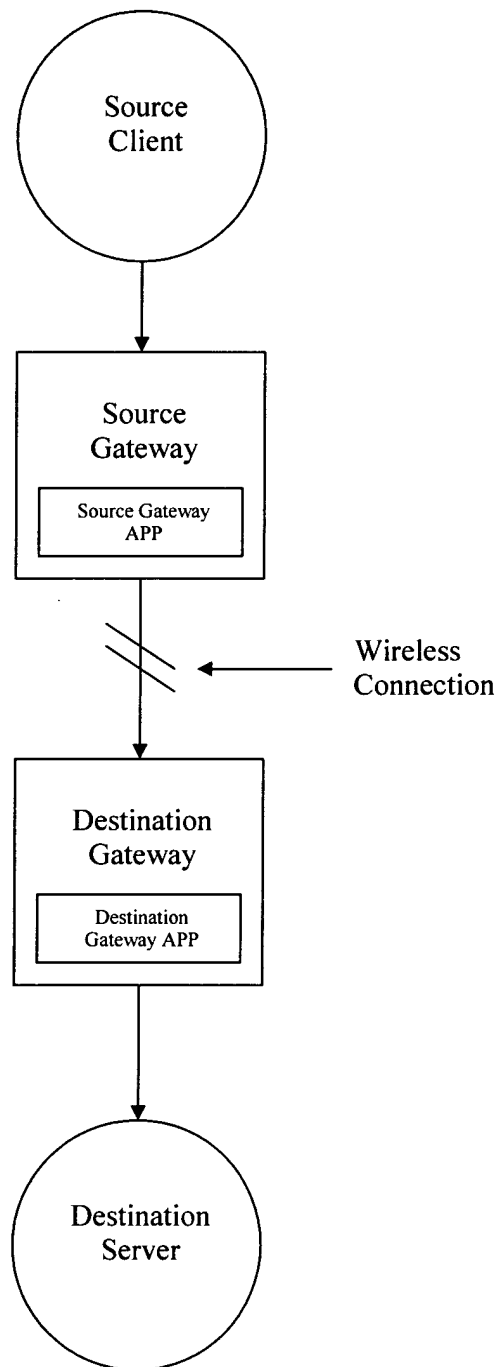
failed to establish a *prima facie* case of anticipation of pending claims 1-33. Reconsideration and allowance of the claims are therefore respectfully solicited.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 1 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 1 (Claims 1, 17, and 33).

Claims 1, 17, and 33 have been rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. However, Applicants submit that the pending claims distinguish quite substantially over *Gelman*.

In summary, *Gelman* teaches communication between a source client and a destination server through an intermediary source gateway and destination gateway. The source client communicates through a *terrestrial* connection to the source gateway by sending a packet using a first protocol, e.g. transmission control protocol (TCP). The source gateway translates the first protocol to a second *wireless* link protocol (WLP) and sends the packet to a destination gateway. The destination gateway converts the packet back to TCP and forwards it on to the destination server.

Thus, what Gelman actually pertains to is a simple translation scheme similar to that used in phone services, where communications appear to be ground based but may actually be wireless at some point in the communication path. A simplified diagram of the *Gelman* invention is presented below (see *Gelman* FIG. 1 for a similar figure consistent with the figure below):



With respect to the *Gelman* reference, it is clear that a communication is transmitted along a singular path with each node in the path simply passing the communication onto the next node until it reaches its destination. Applicants' invention, however, involves redirection of a communication to an out-of-path access controlling web server which communicates *back* to the in-path gateway to instruct it to either grant or deny access over the path. Please direct your attention to Applicants' FIG. 3, reproduced above, for comparison.

The Applicants' invention clearly distinguishes over the teachings of *Gelman*; in the invention the packet is redirected to an access controlling web server that determines whether access to the desired resource is allowable. The access controlling web server is not a link in the path to the desired resource—rather it sends a response to the gateway, informing the gateway whether to allow or disallow access to the desired resource. Thus, in more generalized terms, a packet is sent to a node which does not forward the packet on to a further node in the communications chain, but instead sends a response *back* to an entity in the chain to command *it* to grant or deny access along the path. As noted above, *Gelman* does not teach sending a packet outside the direct transmission path to determine whether to grant or deny access.

As stated in MPEP § 2131, “‘A claim is anticipated only if each and every element as set forth in the claim is found ... in a single prior art reference.’ *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631.” Claim 1 is not anticipated under 35 U.S.C. § 102(e) by *Gelman* since most elements of claim 1 are not taught by *Gelman*.

For your convenience, claim 1 is reproduced below:

1. A method of controlling at a gateway computing device access of a client machine to a desired resource hosted on a destination server, the desired resource being of at least one material type selected from the group including audible materials, readable materials, and viewable materials, comprising the steps of:

(a) at the gateway computing device receiving handshaking packets from the client machine having as a destination address the destination server;

(b) redirecting network communications at the gateway computing device, including the steps of:

redirecting the handshaking packets by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server that is remote from the client, the gateway, and the destination server;

receiving a content request packet from the client machine at the gateway destined for the destination server intended to retrieve the desired resource from the destination server; and

at the gateway redirecting the content request packet by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

(c) receiving a response at the gateway from the access controlling web server; and

(d) at the gateway, controlling access of the client machine to the desired resource based on the response from the access controlling web server, including refusing the client machine access to the desired resource if the response from the access controlling web server indicates that the client should not have access to the desired resource and granting the client machine access to the desired resource if the response from the access controlling web server indicates that the client should have access to the desired resource.

Regarding element (c), *Gelman* does not disclose **any** access controlling entity, especially not an access controlling web server that **controls** access through an in-path gateway rather than simply **conducting** communications. Thus, *Gelman* cannot disclose the step of “receiving a **response** at the gateway **from** the access controlling web server” as required by claim 1. While *Gelman* discloses a gateway and a server as pointed out by the Office in col. 7 lines 10-38, the term “server” is defined in this same section of text as either of nodes 10 or 18 as shown in FIG. 1 of *Gelman* depending on which direction the communication is traveling. Thus, the server referred to in this section of *Gelman* is the destination server (see col. 7 lines

30-34), which clearly cannot be the access controlling web server of claim 1 because element (b) of claim 1 states that the “access controlling web server ... is remote from the client, the gateway, and the destination server.”

Moreover, as element (d) discloses, the gateway controls access to the desired resource based on the response from the access controlling web server. This is not taught by *Gelman*'s automatic repeat request (ARQ) algorithm ARQ messages as contended by the Office. For further details on how *Gelman* uses the ARQ algorithm, please see col. 5 lines 13-21 and col. 2 line 64-col.3 line 7. In summary, the ARQ algorithm is used to maintain reliability by facilitating the retransmission of packets that were not properly received-- it is not used to grant or deny access as expressly required by the claim. For example, by the time the ARQ algorithm becomes relevant, the packet in question has *already* been passed on at least once, so access is clearly not an issue addressed by ARQ.

The Office action notes that *Gelman* mentions firewalls. However, although firewalls generally can be used to restrict access, nowhere does *Gelman* teach a that firewall is or can be used as the gateway or access controlling web server in claim 1. *Gelman* does not disclose any type of server or controller that is outside the direct path of communication between the source and the desired destination.

In summary, it is respectfully submitted that claim 1 is not anticipated by *Gelman* since the reference fails to teach many of the claimed elements. Accordingly, it is respectfully requested that claim 1 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejection thereof.

With respect to independent claims 17 and 33, these claims are said to be rejected for the same reasons as claim 1. Accordingly, the remarks above with respect to claim 1 are also relevant to claims 17 and 33. Claims 17 and 33 are patentable for the same reasons set forth

with respect to claim 1. Accordingly, it is respectfully requested that claims 17 and 33 also be favorably reconsidered.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 2 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 2 (Claims 2 and 18).

Claims 2 and 18 have been rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. However, Applicants again submit that the pending claims distinguish quite substantially over *Gelman*.

Claim 2 recites as follows:

The method according to claim 1, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

The Examiner rejected this claim with the following statement: “...Gelman discloses establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.” Note that the underlined portion of the claim exactly matches the underlined portion of the rejection – the rejection simply parrots the claim with no support at all for the assertion of anticipation. For example, what is the *Gelman* “response” that is being referred to? The rejection of parent claim 1 cites Gelman 7:10-38 as teaching such a response, but this is clearly erroneous-- the cited section merely takes for granted that a connection will be established. In short, the Examiner has not pointed to anything in the reference that would teach the recited limitations, nor have Applicants been able to identify anything remotely anticipatory in the reference.

In summary, it is respectfully submitted that claims 2 and 18 are not anticipated by *Gelman* since the reference fails to teach any of the claimed elements. Accordingly, it is

respectfully requested that claims 2 and 18 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 3 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 3 (Claims 3, 6, 13, 19, 22, and 29).

Claims 3, 6, 13, 19, 22, and 29 as well have been rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. However, Applicants again submit that the pending claims distinguish quite substantially over *Gelman*.

Claim 3 recites as follows:

The method according to claim 2, wherein the content request packet comprises a GET URL packet.

The Examiner rejected this claim by stating that *Gelman* teaches that the content request packet operated on as in parent claims 1 and 2 comprises a GET URL packet. However, again, this is not consistent with the reference. Not only does *Gelman* not teach that a GET URL packet is to be processed as recited in the claims—*Gelman* doesn't mention a GET URL packet at all!

In summary, it is respectfully submitted that claims 3, 6, 13, 19, 22, and 29 are not anticipated by *Gelman* since the reference fails to teach any of the claimed elements. Accordingly, it is respectfully requested that claims 3, 6, 13, 19, 22, and 29 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 4 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 4 (Claims 4 and 20).

Claims 4 and 20 as well have been rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. However, Applicants again submit that the pending claims distinguish quite substantially over *Gelman*.

Claim 4 recites as follows:

The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

The Examiner rejected this claim by stating that “*Gelman* discloses the response indicates that access to the desired resource is allowable if the access controlling webserver does not recognize the URL of the GET URL packet as an inherent feature of the authorization server. This rejection raises several questions: (1) What response? (2) What GET URL packet? (3) What authorization server? These questions have been dealt with above, and would, even alone, tend to indicate that reversal of these rejections is necessitated. But in addition, the rejection simply makes a bald assertion of inherency regarding how the GET URL packet would have been treated by *Gelman*. Aside from the fact that no GET URL packet is even mentioned in the reference, the Applicants previously requested that some foundation or reasoning for inherency other than a bald statement be given, but the advisory action was silent on this issue.

Regarding rejections based upon inherency, MPEP § 2112(IV) states that:

“In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic **necessarily** flows from the teachings of the applied prior art.” *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (underline emphasis in original, bold emphasis added).

Despite Applicants’ request, the Examiner has continually failed to provide a basis in fact and/or technical reasoning as to why the elements recited in these claims necessarily flow

from the teachings of *Gelman*. In fact, there is no reasoning or indication as to how the elements would or even could flow from *Gelman*.

In summary, it is respectfully submitted that claims 4 and 20 are not anticipated by *Gelman* since the reference fails to teach any of the claimed elements. Accordingly, it is respectfully requested that claims 4 and 20 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 5 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 5 (Claims 5 and 21).

Claims 5 and 21 stand rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*.

Applicants again submit that the pending claims distinguish quite substantially over *Gelman*.

Claim 5 recites as follows:

The method according to claim 4, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

In rejecting this claim, the Examiner again flatly stated that the recited combination of elements is an inherent feature of the “authorization server,” presumably of *Gelman*. Again, one has to ask: (1) What response? (2) What GET URL packet? (3) What authorization server? Moreover, this rejection too simply makes a bald assertion of inherency. And again, the Applicants previously requested that some foundation or reasoning for inherency other than a bald statement be provided as required by the MPEP, but the advisory action remained silent on the issue.

Thus, the Examiner has been silent on the reasoning behind his inherency assertions, even when the Applicants affirmatively submitted that the recited limitations are not inherent

or even reasonably inferred from the teachings of *Gelman*. Accordingly, it is respectfully requested that claims 5 and 21 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 6 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 6 (Claims 8, 15, 24, and 31).

Claims 8, 15, 24 and 31 stand rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. Applicants again submit that the pending claims distinguish over *Gelman*.

Claim 8 recites as follows:

The method according to claim 6, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

In rejecting this claim as well, the Examiner simply stated that the recited combination of elements is an inherent feature of “communication between gateway and authorization server.” As with other inherency rejections, Applicants previously requested that some foundation or reasoning for inherency be provided as required by the MPEP, but the advisory action remained silent on the issue.

Thus, the rejections do not meet the requirements of the law or the MPEP, and it is respectfully requested that claims 8, 15, 24 and 31 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 7 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 7 (Claims 9, 16, 25 and 32).

Claims 9, 16, 25 and 32 stand rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. Applicants again submit that the pending claims distinguish quite substantially over *Gelman*.

Claim 9 recites as follows:

The method according to claim 8, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

Again, in rejecting this claim the Examiner simply stated that the recited combination of elements is an inherent feature of “communication between gateway and authorization server.” As with other inherency rejections, Applicants previously requested that some foundation or reasoning for inherency be provided as required by the MPEP, but the advisory action remained silent on the issue.

Thus, the rejections do not meet the requirements of the law or the MPEP, and it is respectfully requested that claims 9, 16, 25 and 32 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 8 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 8 (Claims 10, 11, 26 and 27).

Claims 10, 11, 26 and 27 stand rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. Applicants again submit that the pending claims distinguish over *Gelman*.

Claim 10 recites as follows:

The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

Again, in rejecting the claims of this group the Examiner simply stated that the recited combination of elements is an inherent feature of “communication between gateway and authorization server ” or of “authorization server process.” However, as with the “authorization server,” Gelman also fails to teach the alleged “authorization server process.” In addition, as with the other inherency rejections, Applicants previously requested that a foundation or reasoning for the assertion of inherency be provided as required by the MPEP, but the advisory action remained silent on the issue.

Thus, the rejections do not meet the requirements of the law or the MPEP, and it is respectfully requested that claims 10, 11, 26 and 27 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 9 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 9 (Claims 12 and 28).

Claims 12 and 28 stand rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. Applicants again submit that the pending claims distinguish over *Gelman*.

Claim 12 recites as follows:

The method according to claim 11, wherein the access controlling web server is an RSACi Web Server.

In rejecting the claims of this group the Examiner simply stated that “the access controlling web server is an RSACi Web Server as inherent feature of Web server.” As with the other inherency rejections, Applicants previously requested that a foundation or reasoning

for the assertion of inherency be provided as required by the MPEP, but the advisory action remained silent on the issue.

Thus, the rejections do not meet the requirements of the law or the MPEP, and it is respectfully requested that claims 12 and 28 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

A Prima Facie Case of Anticipation Has Not Been Made With Respect to the Claims of Group 10 Since Gelman Fails To Teach Or Suggest All of the Limitations of the Claims of Group 10 (Claims 7, 14, 23 and 30).

Claims 7, 14, 23 and 30 stand rejected under 35 U.S.C. § 102(e) as anticipated by *Gelman*. Applicants again submit that the pending claims distinguish over *Gelman*.

Claim 7 recites as follows:

The method according to claim 6, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.


The rejection of these claims admits that *Gelman* fails to anticipate the claims, however since the claim remains rejected Applicants have assumed that the action was meant to be worded so as to reject the claims based on inherency. And as with the other inherency rejections, Applicants previously requested that a foundation or reasoning for the assertion of inherency be provided as required by the MPEP, and the advisory action remained silent on the issue.

Thus, the rejections do not meet the requirements of the law or the MPEP, and it is respectfully requested that claims 7, 14, 23 and 30 be favorably reconsidered, and that the Examiner be instructed to withdraw the rejections thereof.

Conclusion: Claims 1-33 Are In Condition For Allowance

This is a case of the Examiner trying to turn a lead wheel weight into a gold brick. The cited reference has nothing to do with the invention other than that both pertain to the known technology of network address translation (NAT). The claims recite specific elements, and almost all of these elements are simply missing from the cited art. In view of the above, the Applicants respectfully submit that claims 1-33 are in condition for allowance. Consideration of this Appeal, removal of the outstanding grounds of rejection, and allowance of claims 1-33 are respectfully solicited.

Respectfully submitted,



Phillip M. Pippenger, Reg. No. 46,055
One of the Attorneys for Applicant(s)
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: April 11, 2005



In re Appln. of Lamb, et al.
Application No. 09/489,629

APPENDIX A: Claims at Issue

Listing of Claims:

1. A method of controlling at a gateway computing device access of a client machine to a desired resource hosted on a destination server, the desired resource being of at least one material type selected from the group including audible materials, readable materials, and viewable materials, comprising the steps of:

- (a) at the gateway computing device receiving handshaking packets from the client machine having as a destination address the destination server;
- (b) redirecting network communications at the gateway computing device, including the steps of:

- redirecting the handshaking packets by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server that is remote from the client, the gateway, and the destination server;

- receiving a content request packet from the client machine at the gateway destined for the destination server intended to retrieve the desired resource from the destination server; and

- at the gateway redirecting the content request packet by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

- (c) receiving a response at the gateway from the access controlling web server; and

- (d) at the gateway, controlling access of the client machine to the desired resource based on the response from the access controlling web server, including refusing the client machine access to the desired resource if the response from the access controlling web server indicates that the client should not have access to the desired resource and granting the client machine access to the desired resource if the response from the access controlling web server indicates that the client should have access to the desired resource.

2. The method according to claim 1, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

3. The method according to claim 2, wherein the content request packet comprises a GET URL packet.

4. The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

5. The method according to claim 4, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

6. The method according to claim 5, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

7. The method according to claim 6, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

8. The method according to claim 6, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

9. The method according to claim 8, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

10. The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

11. The method according to claim 10, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response indicates that the access controlling web server does not recognize the URL of the GET URL packet.

12. The method according to claim 11, wherein the access controlling web server is an RSACi Web Server.

13. The method according to claim 11, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

14. The method according to claim 13, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

15. The method according to claim 13, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

16. The method according to claim 15, wherein the step of determining whether to redirect network communications comprises deciding to redirect network

communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

17. A computer-readable medium having computer-executable instructions for controlling access at a gateway computer of a client computer to a desired resource hosted on a destination server comprising the steps of:

(a) receiving handshaking packets at the gateway computer from the client machine having as a destination address an address corresponding to the destination server;

(b) redirecting network communications at the gateway computer, including the steps of:

redirecting the handshaking packets by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server that is remote from the gateway computer;

receiving a content request packet from the client machine destined for the destination server intended to retrieve the desired resource from the destination server; and

redirecting the content request packet by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

(c) receiving a response at the gateway computer from the access controlling web server; and

(d) at the gateway computer, controlling access of the client machine to the desired resource based on the response from the access controlling web server by granting access if the response indicates that the client may access the desired resource and denying access if the response indicates that the client may not access the desired resource.

18. The computer-readable medium of claim 17, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

19. The computer-readable medium of claim 18, wherein the content request packet comprises a GET URL packet.

20. The computer-readable medium of claim 19, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

21. The computer-readable medium of claim 20, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

22. The computer-readable medium of claim 19, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

23. The computer-readable medium of claim 22, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

24. The computer-readable medium of claim 22, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

25. The computer-readable medium of claim 24, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

26. The computer-readable medium of claim 19, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

27. The computer-readable medium of claim 26, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response indicates that the access controlling web server does not recognize the URL of the GET URL packet.

28. The computer-readable medium of claim 27, wherein the access controlling web server is an RSACi Web Server.

29. The computer-readable medium of claim 27, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

30. The computer-readable medium of claim 29, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

31. The computer-readable medium of claim 29, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

32. The computer-readable medium of claim 31, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

33. In a computer network environment comprising a client, a hosting server, an access controlling server, and a gateway interposed between the client and both of the hosting server and the access controlling server, a method of controlling access of the client to a desired resource hosted on the hosting server, comprising the steps of:

- (a) receiving at the gateway a request packet from the client for the desired resource and redirecting the request packet to the access controlling server;
- (b) receiving at the gateway a permission notification from the access controlling server in response to the redirected request packet; and
- (c) choosing to either grant or deny access of the client machine to the desired resource based on at least one criterion including the content of the permission notification received from the access controlling server.